dprive
Internet-Draft
Intended status: Standards Track
Expires: September 12, 2019

H. Zhang
P. Aras
Salesforce
W. Toorop
NLnet Labs
S. Dickinson
Sinodun IT
A. Mankin
Salesforce

March 11, 2019

DNS Zone Transfer over TLS
draft-hzpa-dprive-xfr-over-tls-00

Abstract

DNS zone transfers are transmitted in clear text, which gives attackers the opportunity to collect the content of a zone by eavesdropping on links. The DNS Transaction Signature (TSIG) is specified to restrict direct zone transfer to authorized clients, but it does not add confidentiality. This document specifies use of TLS to prevent zone collection

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 12, 2019.

Table of Contents

1. Introduction

DNS has a number of privacy vulnerabilities, as discussed in detail in [RFC7626]. Query privacy has received the most attention. There are now standards for three encryption capabilities for queries and more work going on to guide deployment [RFC7858] [RFC8484].

[RFC7626] established that the query transactions are not public and needed protection, but on zone transfer it says only: Privacy risks for the holder of a zone (the risk that someone gets the data) are discussed in [RFC5936] and [RFC5155].

In what way is exposing the full content of a zone a privacy risk? The contents of the zone could include information such as names of persons used in names of hosts. Best practice is not to use personal information for domain names, but many such domain names exist. There may also be regulatory or other reasons why the zone content in full must be treated as private.

Neither of the RFCs mentioned by RFC7626 contemplates the risk that someone gets the data through link eavesdropping.

[RFC5155] specifies NSEC3 to prevent zone enumeration, which is when queries for the authenticated denial of existences records of DNSSEC allow a client to walk through the entire zone. Note that the need for this protection also motivates NSEC5; zone walking is now possible with NSEC3 due to crypto-breaking advances, and NSEC5 is a response to this problem.

[RFC5155] does not address data obtained outside zone enumeration (nor does NSEC5). Preventing eavesdropping of zone transfers (this draft) is orthogonal to preventing zone enumeration, though they aim to protect the same information.

[RFC5936] specifies using TSIG [RFC2845] for authorization of the clients of a zone transfer and for data integrity, but does not express any need for confidentiality, and TSIG does not offer encryption. Some operators use SSH tunneling or IPSEC to encrypt the transfer data. Because the AXFR zone transfer is carried out over TCP from DNS protocol implementations, encrypting AXFR using DNS over TLS [RFC7858], aka DOT, seems like a simple step forward. This document specifies how to use DOT to prevent zone collection from zone transfers, including discussion of approaches for IXFR, which uses UDP or TCP.

Next steps: work on questions at DNS table during Hackathon, expand this draft, then solicit discussion on the DPRIVE mailing list.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Privacy terminology is as described in Section 3 of [RFC6973].

DNS terminology is as described in [RFC8499]:

3. Zone Transfer Confidentiality Overview

4. Zone Transfer with DOT - Authentication

Subsection - TSIG

Subsection - Mutual TLS

5. Session Establishment and Closing

Subsection - AXFR Sessions

The connection flow in AXFR is a NOTIFY from the primary server to the secondary server, and then an AXFR request from the secondary to the primay after which the data flows.

The connection for AXFR SHOULD be established using port 853, as specified in [RFC7858]. If there is no response on port 853, the connection MAY be attempted using port 443.

TODO: diagram of connection flow for AXFR, without and with DOT

Subsection - IXFR Sessions (?)

[RFC1995] specifies that Incremental Transfer may use UDP if the entire IXFR response can be contained in a single DNS packet, otherwise, TCP is used.

Given this, how should confidentiality of IXFR be provided? To discuss: should IXFR have a mode in which TCP is mandatory? or should there be an approach of starting with DNS over DTLS, and switching to DNS over TLS with a TCP switch? In workloads where there are frequent IXFRs, is the persistent mode that TCP-Mode would enable (as well as the retries, a benefit?

Subsection - Policies for Both AXFR and IXFR

In order to assure the confidentiality of the zone information, all the servers (primary and secondary) MUST have a consistent confidentiality use. If any do not, this is a weak link for attackers to exploit. How to do this is TBD.

The entire group (the primary and all secondaries) MUST have a consistent policy on Strict or Non-Strict mode of operation. How to do this is TBD.

Subsection - Next Steps

Upcoming open hackathon experiments will feed into this Session Establishment and Closing section, as much about this needs exploration as well as dicussion on the mailing list.

6. Performance Considerations

The details in [RFC7858] about using persistent connections and TLS Session Resume are fully applicable to DNS Transfer over DOT as well.

7. Implementation Considerations

TBA

8. IANA Considerations

TBD

9. Security Considerations

This document specifies a security measure against a DNS risk, the risk that an attacker collects entire DNS zones through eavesdropping on plaintext DNS zone transfers. It presents a new Security Consideration for DNS. Some questions to discuss are: should DOT in this new case be required to use only TLS1.3 and higher to avoid residual exposure? How should padding be used (if it should)?

10. Acknowledgements

Benno, Shumon, Tim

11. Contributors

The following contributed significantly to the document:

12. Changelog

draft-hzpa-dprive-xfr-over-tls-00

o Initial commit

13. References

13.1. Normative References

[I-D.bortzmeyer-dprive-rfc7626-bis]
Bortzmeyer, S. and S. Dickinson, "DNS Privacy Considerations", draft-bortzmeyer-dprive-rfc7626-bis-02 (work in progress), January 2019.

[I-D.dickinson-dprive-bcp-op]
Dickinson, S., Overeinder, B., Rijswijk-Deij, R., and A. Mankin, "Recommendations for DNS Privacy Service Operators", draft-dickinson-dprive-bcp-op-01 (work in progress), July 2018.

[RFC1995] Ohta, M., "Incremental Zone Transfer in DNS", RFC 1995, DOI 10.17487/RFC1995, August 1996, <https://www.rfc-editor.org/info/rfc1995>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake 3rd, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, DOI 10.17487/RFC2845, May 2000, <https://www.rfc-editor.org/info/rfc2845>.

[RFC5077] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 5077, DOI 10.17487/RFC5077, January 2008, <https://www.rfc-editor.org/info/rfc5077>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/info/rfc5155>.

[RFC5936] Lewis, E. and A. Hoenes, Ed., "DNS Zone Transfer Protocol (AXFR)", RFC 5936, DOI 10.17487/RFC5936, June 2010, <https://www.rfc-editor.org/info/rfc5936>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <https://www.rfc-editor.org/info/rfc7525>.

[RFC7626] Bortzmeyer, S., "DNS Privacy Considerations", RFC 7626, DOI 10.17487/RFC7626, August 2015, <https://www.rfc-editor.org/info/rfc7626>.

[RFC7766] Dickinson, J., Dickinson, S., Bellis, R., Mankin, A., and D. Wessels, "DNS Transport over TCP - Implementation Requirements", RFC 7766, DOI 10.17487/RFC7766, March 2016, <https://www.rfc-editor.org/info/rfc7766>.

[RFC7830] Mayrhofer, A., "The EDNS(0) Padding Option", RFC 7830, DOI 10.17487/RFC7830, May 2016, <https://www.rfc-editor.org/info/rfc7830>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <https://www.rfc-editor.org/info/rfc8310>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8467] Mayrhofer, A., "Padding Policies for Extension Mechanisms for DNS (EDNS(0))", RFC 8467, DOI 10.17487/RFC8467, October 2018, <https://www.rfc-editor.org/info/rfc8467>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

13.2. Informative References

[NSEC5Research]
Goldberg, S., Naor, M., Papadopoulos, D., and L. Reyzin, "NSEC5: Provably Preventing DNSSEC Zone Enumeration", 2015, <https://www.ndss-symposium.org/ndss2015/ndss-2015-programme/nsec5-provably-preventing-dnssec-zone-enumeration/>.

[RFC7129] Gieben, R. and W. Mekking, "Authenticated Denial of Existence in the DNS", RFC 7129, DOI 10.17487/RFC7129, February 2014, <https://www.rfc-editor.org/info/rfc7129>.

[RFC7816] Bortzmeyer, S., "DNS Query Name Minimisation to Improve Privacy", RFC 7816, DOI 10.17487/RFC7816, March 2016, <https://www.rfc-editor.org/info/rfc7816>.

[RFC7871] Contavalli, C., van der Gaast, W., Lawrence, D., and W. Kumari, "Client Subnet in DNS Queries", RFC 7871, DOI 10.17487/RFC7871, May 2016, <https://www.rfc-editor.org/info/rfc7871>.

[RFC7873] Eastlake 3rd, D. and M. Andrews, "Domain Name System (DNS) Cookies", RFC 7873, DOI 10.17487/RFC7873, May 2016, <https://www.rfc-editor.org/info/rfc7873>.

[RFC8094] Reddy, T., Wing, D., and P. Patil, "DNS over Datagram Transport Layer Security (DTLS)", RFC 8094, DOI 10.17487/RFC8094, February 2017, <https://www.rfc-editor.org/info/rfc8094>.

Authors' Addresses

Han Zhang
Salesforce
San Francisco, CA
United States

Email: hzhang@salesforce.com

Pallavi Aras
Salesforce
Herndon, VA
United States

Email: paras@salesforce.com

Willem Toorop
NLnet Labs
Science Park 400
Amsterdam Amsterdam 1098 XH
The Netherlands

Email: willem@nlnetlabs.nl

Sara Dickinson
Sinodun IT
Magdalen Centre
Oxford Science Park
Oxford OX4 4GA
United Kingdom

Email: sara@sinodun.com

Allison Mankin
Salesforce
Herndon, VA

Email: allison.mankin@gmail.com